Notebooks

Sicher hinter Schloss und Riegel

Wie die Computerwoche 1/2005 berichtet, werden Notebooks immer populärer und sind aus dem EDV-Alltag von Betrieben und Behörden nicht mehr wegzudenken. Sie führen wie USB-Sticks aber auch zu neuen Gefahren und Risiken, da auf der Festplatte des Notebooks interne Daten den Betrieb oder die Behörde verlassen.

Immer wieder hört man von abhanden gekommenen Notebooks. Selbst Polizeibehörden und sensible Bereiche von Ministerien sind davon nicht verschont geblieben.

Achten Sie darauf, dass der Bootschutz auf jeden Fall aktiviert ist

Während beim Desktop-Rechner nur die wenigsten einen Bootschutz – in der Regel ein BIOS-Passwort – aktiviert haben, ist dieser Schutz bei einem Notebook unerlässlich. Nur so können Sie verhindern, dass jedermann das Notebook startet. Das Argument, dass ja das Betriebssystem eine Passwortabfrage habe, ist nichtig, da bei einem nicht vorhandenen Bootschutz auch von CD, Floppy oder gar USB-Stick gebootet werden kann.

Ein weiterer Schutz ist ein fest eingebauter Chipkartenleser

Etliche aktuelle Notebooks bieten bereits einen fest eingebauten Chipkartenleser. Damit bootet das Notebook bei geeigneter Konfiguration nur mit der richtigen Chipkarte im Leser.

Die Daten auf der Festplatte müssen verschlüsselt sein

Auf der Festplatte des Notebooks sind in Form von Textverarbeitungsdateien, Tabellenkalkulationsdateien, Datenbanken, E-Mail und vielen anderen Formen sowohl personenbezogene als auch andere vertrauliche Daten gespeichert. Der Dieb eines Notebooks kann Schutzmaßnahmen wie Bootschutz umgehen, indem er die Festplatte des Notebooks aus- und dann in einen anderen Rechner einbaut und dort ausliest. Dagegen hilft nur die vollständige Verschlüsselung der Daten auf der Festplatte.

Ohne Passwort auch kein Zugang zu den entschlüsselten Daten

Bewährt haben sich Produkte wie z.B. Utimaco Safeguard Easy, die die komplette Festplatte verschlüsseln und dadurch einen sicheren Bootschutz gewährleisten können. Ohne Eingabe des richtigen Passworts wird die Festplatte nicht entschlüsselt, und das Notebook bootet nicht. Nur mit derartigen Programmen kann die Auslagerungsdatei verschlüsselt werden.

Überprüfen Sie, ob folgende Sicherheitsmaßnahmen vorhanden sind:

- Bootschutz
- Datenverschlüsselung
- Personal Firewall
- Aktueller Virenschutz
- Aktueller Dialerschutz
- VPN-Software
- Kensington-Schloss
- Patchmanagement

Überprüfen Sie, ob ein aktueller Virenscanner installiert ist

Notebooks werden unterwegs an Netze angeschlossen, sowohl direkt über die Netzwerkkarte per LAN oder DSL als auch über Modem oder ISDN-Karte per DFÜ-Netzwerk. Damit befinden sie sich im Internet oder in einer fremden Umgebung ohne Schutz der Unternehmens-Firewall.

Je nach Konfiguration ist es sinnvoll, eine Personal Firewall zu installieren. Ihr Einsatz sollte allerdings nicht dazu verleiten, das Notebook nachlässig zu konfigurieren.

Mit Verschlüsselungssoftware sicher „nach Hause telefonieren“

Für Datenverbindungen in die Sicherheitszonen des Betriebs ist eine Verschlüsselungssoftware erforderlich. Die Firmenpolicy schreibt vor, welcher Zugang erlaubt ist. Je nach Möglichkeit muss die geeignete Software installiert und konfiguriert sein. Achten Sie auch darauf, dass die Konfiguration von extern getestet wurde und die Benutzer in die teilweise komplexe Bedienung eingewiesen sind.

Notebooks sollten auch physisch mit einem Schloss gesichert sein

Zur Grundausstattung eines Notebooks gehört ein Schloss mit Kette oder Stahlseil (Kensigton-Schloss „Microsaver“). Auch wenn sich diese mit entsprechendem Werkzeug aufschneiden lassen, bieten sie doch Schutz vor dem „schnellen Diebstahl“.

Das Wichtigste ist die Verschlüsselung

Mit entsprechenden Sicherheitsmaßnahmen, wovon Verschlüsselung die wichtigste ist, kann auch ein Notebook verantwortungsbewusst außerhalb des Unternehmens betrieben werden. Trotz aller technischen Maßnahmen bleibt allerdings der Nutzer ein Schwachpunkt.

Es sollten einfache Verhaltensregeln vorhanden und bekannt – am besten in Form einer Nutzungserklärung auch unterschrieben – sein, wie z.B. das Notebook im Kofferraum einzuschließen und es nicht auf den Rücksitz zu legen. Dies hilft, dem Diebstahl der Hardware und der Information vorzubeugen.

Checken Sie, ob für Notebooks immer alle aktuellen Sicherheitsupdates vorgesehen sind. Die Installation muss unmittelbar nach der Bereitstellung erfolgen. Auch ein sicherer Browser wie der „Firefox“ ist zu empfehlen.

Prof. Dr. Rainer W. Gerling